Science and technology

Landman, Lennart

Published in:
Clingendael 2013 Strategic Monitor

9

Science and technology

Lennart Landman

Introduction

The 2012 Strategic Monitor predicted that in the area of science and technology, the dominance of (Western) state actors would shift towards non-Western and non-state actors. New technology is increasingly being commercially developed and is freely available to all players, as the previous report concluded. Yet state actors are still dominant in some areas, such as space. From this diffuse image, the 2012 Strategic Monitor noted a shift towards the fragmentation scenario and for that reason placed science and technology in the fragmentation quadrant. The developments outlined in the previous edition appear to have partially continued in the past year. However, there have also been a number of significant changes. In this chapter, we will reassess the conclusions of the 2012 Strategic Monitor based on the latest developments in science and technology.

1 Significant changes in the past year

The developments of the past year showed a trend towards fragmentation as well as some elements in the direction of a greater role for the state. The overall picture is therefore quite diffuse.

Developments in recent years have broadened the freedom of access to new technologies and knowledge for non-state actors. 3D printers that produce objects in plastics are now being sold for anywhere between several hundreds to thousands of euros. As a result, print products are becoming publicly available. In open-access online libraries, design files of a growing number of parts and complete products are publicly shared. In the past year, certain open-source projects received much attention for developing designs for a handgun and for a self-replicating 3D printer.

In the digital domain, hacktivists remained active in 2012, extending the trend of growing cyber crime (Symantec; Sophos 2012). State-sponsored digital attacks have increased in the past year, but identifying the culprits remains difficult. It is suspected that recent attacks on the energy sectors of countries such as Iran, Saudi Arabia, Qatar, the US, Canada, and Vietnam are the work of state-sponsored actors, although to date, hard evidence is lacking. Such attacks aim to both steal information and Research and Development (R&D) designs (cyber espionage) and disable systems (cyber sabotage). In addition to companies, military organisations, ministries, and think tanks in primarily Western—but also non-Western countries—have been targeted in the past year. Often, the work of Chinese hackers is suspected, although Russia, Iran, Israel, and the United States are also likely to have been active in this area in 2012.

Although digital security was discussed in various international forums over the past year, a common conceptual framework and shared norms are still lacking. No concrete progress has been made in the area of an international cyber security convention. At the national level, states have expanded their (integrated) digital security policy and thus

Box 1 **The increasing complexity and impact of cyber crime**

The complexity of viruses and attacks has increased rapidly in recent years. These types of crime focus on such things as stealing credit card data and plundering online bank accounts. In addition, private data has become an increasingly popular target. Especially individual consumers and their mobile devices remain a weak link in the protection against cyber crime. In early 2013, the US Cyber Crimes Watch published its annual Cyber Crime Statistics. The report showed that 75 million so-called scam emails are sent every day; that at the global level roughly 65 percent of internet users have had to deal with cyber crime, and that 25 percent of cyber crime remains unsolved.

There are different types of cyber crime. At the global level, malware—better known as malicious software—and computer viruses are the most common form of cyber crime (54 percent), followed by online scams (11 percent) and internet fraud (10 percent), also known as phishing. A recent report published by Norton shows that young people, women, and inhabitants of emerging countries are most at risk of becoming a victim of cyber crime (Norton 2012).

Enormous costs are associated with cyber crime. In the past year alone, the costs due to cyber crime in 24 countries amounted to some 388 billion dollars (Norton 2012).

both their abilities and powers in this area. The control and prevention of cyber crime is currently one of the priorities of governments (see Box 1 for further details).

Several states have worked on legislation in the past year to enable them to exercise control over parts of networks and telecommunications. During the World Conference on International Telecommunications in Dubai, proposals to place internet protocols under the supervision of states were supported by a majority of countries, including Russia, China, the African countries, and countries in the Middle East. In some cases, citizens have opposed such legislation, which in their eyes limits the freedom of the digital world. Protest movements arose against the Stop Online Piracy Act (SOPA), the Protect IP Act (PIPA), and the Anti-counterfeiting Trade Agreement (ACTA).

The field of robotics has developed further. Just as with 3D printers, small commercial drones have become cheaper and more accessible to individuals. More and more states are adding military robots to their arsenals, including both armed and unarmed aircraft (UAVs). The United States has frequently used its UAVs during attacks in Afghanistan, Pakistan, Somalia, and Yemen as well as for operations (including intelligence operations) over the Philippines, Iran, Libya, Mali, and Syria. Non-state actors such as Hamas and drug cartels from Central America have also used UAVs, but the US still leads in the area of military robotics. This year the US launched the first armed unmanned surface vessel.

In the field of space, SpaceX became the first commercial company to supply the space station ISS last year. Continuous development of space drones such as the experimental X-37B (US) and Shenlong (China) is perpetuating multipolar tensions over military space programmes. Commercial non-state space initiatives are developing steadily, but this area continues to be dominated by state actors (with the exception of satellite capacity where commercial parties have a certain presence).

Scenario framework

On the one hand, non-state actors gained influence in the past year. In terms of security policy, they were characterised by non-cooperation, resulting in fragmentation. On the other hand, states tried to enhance their grip on technology issues, whereby the international cooperative element was largely missing. In this sense, a certain degree of multipolarity exists.

2 The next five to ten years: Probabilities and uncertainties

Probabilities

- New technologies will be widely available for both state and non-state actors.
- Government regulation of technology and control of the digital space will likely increase.
- The development of an 'internet of things' makes it more likely that a cyber attack, sabotage, or disruption would have significant social, economic, or military consequences.
- Although with drones, a human operator retains final control, a discussion is likely to arise on the gray area of sanctioned autonomous acts.

Uncertainties

- To what extent will state actors retain their technological superiority in future conflicts, given that non-state actors have access to the same technologies as states?
- Are governments able to regulate and control digital space, and will citizens accept the negative consequences of this?
- Will weapons systems from space—or against targets in space—be used?
- What are the risks of biotechnology and nanotechnology for the human race and the environment?

For the next five to ten years, it is likely that a number of developments in the field of science and technology will continue. This will make new products and applications available, but it can also bring social and international political changes with it. There are also implications for the armed forces (see Box 2).

Box 2 **Armed forces and technology**

Over the past few years, militaries around the world have been downsized, both in terms of materiel and personnel. At the same time, the qualitative capabilities and responsibilities of materiel and personnel have increased, and more and more tasks are being centralised—with the help of technology—by the individual soldier and the weapons platform. In Europe and the US, this trend is reinforced by the pressure of shrinking defence budgets, which gives rise to attempts to get more value for one's money. In the BRICS countries, defence spending has increased in recent years—a trend that is part of the modernisation of their forces.

The defence priorities of the United States will in the coming years be focused on power projection and smaller and more rapidly deployable forces. In concrete terms, they will focus on special operations forces (supported by information and high-tech materiel), maritime capabilities (including unmanned USVs), unmanned or manned long-range surveillance and strike capabilities, and digital warfare. China seems to be following American technological developments closely and has invested in aircraft carriers, stealth aircraft, missile technology, space, drones, and cyber warfare capabilities. Within Europe, the prioritisation is unclear due to the lack of a common strategic vision. European efforts within the EU are likely to focus on limited stabilisation and reconstruction operations that rely less on defence technology.

The gap in military technology between Europe and the US remained large in 2012. Under pressure from spending cuts, modernisation of the armed forces in the EU will probably occur more slowly than in the US, with some small European countries possibly delaying modernisation plans for years to come. This gap could conceivably be reduced in the future through improved European defence cooperation and the development of a common European defence industry. But in times of economic crisis and budget cuts, it is uncertain whether and to what extent the political will for this can be found.

The most likely technological developments are:

- continued robotisation and automation;
- further digitisation;
- increased connectivity to networks;
- increase in numbers and quality of sensors;
- increase of capacity in data aggregation;
- further developments in algorithms and smart software;
- further opportunities in creating and manipulating nano-, bio-, and neurotechnologies.

The above developments will converge and reinforce each other in the coming years, making a number of products and applications—as well as their further implementation—possible.

Sensors for images, sound, temperature, materials analysis, GPS, and generic reprogrammable sensors will probably become cheaper and will be used in a combined fashion in many products, from consumer devices to buildings, roads, and lights. Devices and sensors will increasingly be connected to digital networks, the so-called *internet of things*, allowing large amounts of data to be aggregated. The development of better algorithms and software ensures that these massive data sets (*big data*) can be used to generate (*real-time*) insights. This can involve situational awareness in crisis situations, the optimisation of business processes, or the monitoring of and developing insight into complex ecological, sociological, and social phenomena. As a result, society's vulnerability to failure, malfunction, or deliberate disruption will increase.

These technologies will also be used to automate and robotise more functions. The development of better artificial intelligence and new materials will make more, smaller, more efficient and/or autonomous robotics possible. On the one hand, these will be individual machines designed to take on a single task or a group of tasks. On the other hand, large groups of small machines will work together in swarms to accomplish their task. Military robots will increasingly be automated. Although a human operator will retain ultimate control over the use of force, a discussion is likely to arise on the gray area of sanctioned autonomous acts, especially in combat situations where artificial intelligence yields a greater chance of survival via its quicker and more efficient actions.

In the field of biotechnology and genetic engineering, cheap genome analysis will make more personalised medical treatments possible. Implants and protheses for, amongst others, senses will be improved in the coming years.

Online collaborative networks make it increasingly possible to use the knowledge and skills of the collective via open-source. A growing group of people with internet have access to not only education, advice, software, entertainment but also designs that can be printed out on 3D printers. The 'digital divide' between those who benefit from digital technologies and those who do not will become smaller. However, people without internet access—some 4.6 billion in 2012—will increasingly be at a great social and economic disadvantage.

The digitisation, automation, and robotisation of production and services and the increasing demand for high-tech and digital products and services is resulting in qualitative knowledge becoming more valuable for economic activities (Brynjolfsson 2011). Parts of the industrial design and production processes will be more decentralised to collaborative networks or individuals who generate bottom-up innovation. It is likely that these parts of the production process will be placed closer to the product developer and the consumer. The United States and Europe are strong in terms of knowledge and have large consumer groups, so they are well positioned to benefit from this development. It is uncertain whether the developments expected in the next five to ten years will significantly affect international economic relations. The growing importance of digital production and the portability of digital designs and products is likely to lead to further tensions among companies as well as states regarding the protection of intellectual property against espionage, piracy, and patent infringement.

Soldiers prepare drones on the deck of the USS Tortuga.
Photo: Official US Navy Imagery

In the next decade, technological superiority is likely to become more diffuse. With the further integration of computers, sensors, network connectivity, databases, and artificial intelligence in personal devices, the individual has more and more possibilities within his/her reach. Through digitisation, global marketplaces, and 3D printing, new technologies and products will rapidly become commercially available to a wide audience. Hence, non-state actors will have more opportunities to assert their influence. These developments is likely to strengthen the position of central nodes in networks that have access to large amounts of sensors, information flows, and databases and that have the capacity and resources to transform this information into products and services. Examples include not only Google, IBM, and Huawei but also intelligence services and online criminal syndicates.

As a result of the benefits of automation and big data, more and more elements of the economy and society will *de facto* be run by algorithms that determine optimal choices. The increasing complexity of systems and the issues they deal with will lead to a decline in humans' understanding of, insight into, and control over these systems. Our dependence on these algorithms entails risks of disruption when they crash or when data sets are misinterpreted.

These technological developments cause our dealings with each other to change, while empathy and solidarity are coming under strain (Konrath 2011). The generations growing up in the digital age may be less inclined to conform to contemporary social and political structures and to support the approach to issues of general interest such as ageing and the protection of international law. It is, however, uncertain to what extent this trend will be articulated in the coming years due to the influence of other social and political variables.

Due to technological developments, the social and security challenges that states face are becoming more complex and difficult to control. Partly because of this, states are likely to try to get a better grip on these challenges. Governments will probably attribute more powers to themselves in an attempt to regulate the use of certain technologies. At the same time, technology will also be used for the benefit of governments, for example to support policymaking with data analysis and mathematical models. Also, an increasing number of techniques may be used to monitor parts of society for any undesirable behaviour: this can be large group processes such as riots and mass hysteria or at the individual level, such as recognising patterns of behaviour that are associated with fraud, crime, or terrorism. In the context of national security, governments will collect large amounts of information through social media, the internet, cameras, transactions, and so on.

Attempts by governments to regulate the availability of dangerous technologies such as print weapons, hacker tools, or modified biological and genetic mass are likely to increase. It is also likely that states will expand their powers in the future to safeguard the functioning of critical parts of the digital infrastructure in times of emergency. We cannot rule out the possibility that governments will use means that could also influence the systems of innocent citizens and businesses.

It is uncertain whether these measures are sufficient for states to tackle the increasing influence of (non-cooperative) non-state actors. They also bring up fundamental questions regarding constitutional rights such as due process and privacy. It is uncertain, for example, to what extent the public or politicians will allow the monitoring of behaviour to be applied. Threats will increasingly have a transnational character. State intervention will increasingly be based on bilateral agreements with stakeholder countries but more ideally on multilateral governance agreements and arrangements with civil society and other non-state stakeholders.

Scenario framework

Technology is a catalyst for development and change. Actors that quickly recognise and implement the potential of technological developments can therefore obtain significant advantages. This applies to both cooperative and non-cooperative associations of state and non-state actors. As a result, the main development in the scenario framework for the next five to ten years cannot be estimated with much certainty. Given that non-state actors have in the past shown themselves to be adaptive and states generally change slowly, it is slightly more likely that non-state actors will gain more influence and will be more

non-cooperative than cooperative in the area of security. This means that a movement in the direction of the fragmentation scenario can be expected, although the overall image remains diffuse.

3 Strategic shocks

Strategic shocks

- Western military superiority is neutralised.
- Large-scale failure of information systems and payments systems after a cyber attack.
- A massive Chinese cyber attack on US military networks, satellites, and command centres.
- Development of foolproof digital identification, verification, and traceability.
- Uncontrollable nanotechnology or biotechnology brings widespread and serious damage to people and the environment.

Relative to the previous edition of the Strategic Monitor, a number of strategic shocks within technology and science have remained the same.

Western military superiority is neutralised. Because many new technologies are readily available to various actors—both non-state actors and emerging powers—this shock has become slightly more likely. The military rise of the BRICS, especially China, also contributes to this.

Large-scale failure of information systems and payments systems after a cyber attack. As a result of the increasing integration and digitisation of critical equipment, the vulnerability to this shock has increased. Although this strategic shock is not unlikely, we cannot say much about its probability given the speed with which developments in the digital world are taking place.

A massive Chinese cyber attack on US military networks, satellites, and command centres overwhelms US digital defence and makes the deployment of US armed forces impossible. Although there are warnings in some circles of a digital Pearl Harbor, this shock is not likely.

Development of foolproof digital identification, verification, and traceability. Cyber attacks and crimes can be traced back to the source: cyber crime and 'hacktivism' decline dramatically; states will no longer be able to deny responsibility for a cyber attack, making it occur less frequently, but cyber attacks will have greater political impact. This shock has become somewhat more likely as a result of technological developments and the call for more regulation.

In addition to the strategic shocks already mentioned in the previous Monitor, we have added a new strategic shock: **uncontrollable nanotechnology or biotechnology brings about widespread and serious damage to people and the environment.** This shock has become slightly more likely because these materials are often used, but an incident of catastrophic magnitude seems unlikely.

4 Winners and losers

The winners and losers are among both state and non-state actors, whereby the category of non-state actors in general can be seen as the winner. Cyber criminals have significant leeway, and the profits of cyber crime continue to increase. Drug cartels also understand how to take advantage of technological developments such as drones. Despite the fact that some hacktivists were arrested over the past year, many other hacktivists were able to book successes. This form of activism seems to be gaining legitimacy. Governments are able to implement effective countermeasures only to a limited extent against such non-state actors. States are still losers in the relative sense, and it is uncertain whether this will change in the coming years.

In general, the further development of decentralised and digital production, 3D printers, and open-source information gives the non-state actor more opportunities. Actors who play a central role in networks and big data, such as Google and IBM, can be declared winners. The growing importance of high-quality knowledge in economic activities means that states with a strong knowledge infrastructure have a comparative advantage. Emerging economies using technologies that are available across the world can more rapidly catch up, but states that lag behind are likely to see the economic gap grow. Low-educated people in developed countries run the risk of being left out as their jobs become more and more automated and they are unable to make the transition to new work. The considerable number of people without access to the internet in a world undergoing large-scale digitisation are clear losers.

5 Implications for global security and stability

Developments in the field of science and technology affect larger processes and trends within the global system. First, globalising technologies make it possible for more players to participate in global economic, social, and political structures. Social and economic development, inclusion, and interdependence can have a dampening effect on local and regional instability, but at the same time rapid development can lead to adjustment problems within existing power structures at both the national and international levels. As a result, actors that don't have a technological connection are more intensely hit, causing economic and social disparities to grow and the risk of deprivation and political violence to increase.

In the digital domain, the increase in state-sponsored hackers and offensive military cyber programmes have a potential impact on global stability and security. Norms and regulatory mechanisms for cyber attacks are largely missing, and it is uncertain whether dampening mechanisms that in other cases prevent conflicts from escalating will also work for digital attacks.

The further development of defence technologies such as drones, missile technology, and military space initiatives are a source of tension between China and the United States.

Finally, the vulnerability of societies as a result of digitisation and the dependence on networks has increased. Due to free access to a wide range of technologies, the number of opportunities for non-state actors to pose a threat with limited resources has increased.

A cyber attack could mean that government agencies or national infrastructures are consciously switched off, but viruses can also have unintended effects on other systems at hospitals, banks, utility companies, or individuals. The disruption of critical infrastructure by a large-scale cyber attack can seriously affect national security. The complexity and diversity of systems means not only that there are many vulnerabilities but also that it is harder to simultaneously infiltrate or switch off these various systems on a large scale.

Developments in the field of biological, pharmaceutical, and genetic technology will make more medical treatments possible. These treatments will not necessarily be cheaper or more readily available, which in turn could put greater pressure on the health care system and its financial sustainability. A health care system in which money makes a big difference in longevity and quality can lead to polarisation.

Conclusion

Developments in technology and science continue unabated and seem to be happening more and more rapidly. In the coming years, developments in especially the digital domain will be influential, but also increasingly in nanotechnology, biotechnology, neurotechnology, and genetic technology. In terms of security, digital threats, robotisation, sensors, and artificial intelligence will determine a large part of the future. Technology has the potential to dramatically change social, economic, and international political systems, but it certainly does not stand alone. Social and political choices and processes determine how a new technology is implemented. Non-state actors seem to be very good at exploiting technologies due to their lack of restraint as well as their ability to adapt. The organising power of states remains significant, however, and has so far been able to make technology work to its advantage. In the next five to ten years, the non-alignment of non-state actors and the power of state actors will form an interesting field of tension.